

AMENDMENT TO THE CLAIMS

Please amend the presently pending claims as follows:

1 - 19. (Cancelled)

20. (Previously Presented) A computer implemented process comprising:

obtaining a set of one or more private values  $Q_1, Q_2, \dots, Q_m$  and respective public values  $G_1, G_2, \dots, G_m$ , each pair of values  $Q_i, G_i$  verifying either the equation  $G_i \cdot Q_i^v \equiv 1 \pmod{n}$  or the equation  $G_i \equiv Q_i^v \pmod{n}$ , wherein  $m$  is an integer greater than or equal to 1,  $i$  is an integer between 1 and  $m$ , and wherein  $n$  is a public integer equal to the product of  $f$  private prime factors designated by  $p_1, \dots, p_f$ , at least two of these prime factors being different from each other, wherein  $f$  is an integer greater than 1, and wherein  $v$  is a public exponent such that  $v = 2^k$ , and wherein  $k$  is a security parameter having an integer value greater than 1, and wherein each public value  $G_i$  for  $i = 1, \dots, m$  is such that  $G_i \equiv g_i^2 \pmod{n}$ , wherein  $g_i$  for  $i = 1, \dots, m$  is a base number having an integer value greater than 1 and smaller than each of the prime factors  $p_1, \dots, p_f$ , and  $g_i$  is a non-quadratic residue of the ring of integers modulo  $n$ ;

receiving a commitment  $R$  from a demonstrator, the commitment  $R$  having a value computed such that:  $R = r^v \pmod{n}$ , wherein  $r$  is an integer randomly chosen by the demonstrator;

choosing  $m$  challenges  $d_1, d_2, \dots, d_m$  randomly;

sending the challenges  $d_1, d_2, \dots, d_m$  to the demonstrator;

receiving a response  $D$  from the demonstrator, the response  $D$  having a value computed

such that:  $D = r \bullet Q_1^{d_1} \bullet Q_2^{d_2} \bullet \dots \bullet Q_m^{d_m} \bmod n$ ; and

determining that the demonstrator is authentic if the response  $D$  has a value such that:  $D^v \bullet G_1^{\varepsilon_1 d_1} \bullet G_2^{\varepsilon_2 d_2} \bullet \dots \bullet G_m^{\varepsilon_m d_m} \bmod n$  is equal to the commitment  $R$ , wherein, for  $i = 1, \dots, m$ ,  $\varepsilon_i = +1$  in the case  $G_i \bullet Q_i^v = 1 \bmod n$  and  $\varepsilon_i = -1$  in the case  $G_i = Q_i^v \bmod n$ .

21. (Previously Presented) A computer implemented process comprising:

obtaining a set of one or more private values  $Q_1, Q_2, \dots, Q_m$  and respective public values  $G_1, G_2, \dots, G_m$ , each pair of values  $Q_i, G_i$  verifying either the equation  $G_i \bullet Q_i^v \equiv 1 \bmod n$  or the equation  $G_i \equiv Q_i^v \bmod n$ , wherein  $m$  is an integer greater than or equal to 1,  $i$  is an integer between 1 and  $m$ , and wherein  $n$  is a public integer equal to the product of  $f$  private prime factors designated by  $p_1, \dots, p_f$ , at least two of these prime factors being different from each other, wherein  $f$  is an integer greater than 1, and wherein  $v$  is a public exponent such that  $v = 2^k$ , and wherein  $k$  is a security parameter having an integer value greater than 1, and wherein each public value  $G_i$  for  $i = 1, \dots, m$  is such that  $G_i \equiv g_i^2 \bmod n$ , wherein  $g_i$  for  $i = 1, \dots, m$  is a base number having an integer value greater than 1 and smaller than each of the prime factors  $p_1, \dots, p_f$ , and  $g_i$  is a non-quadratic residue of the ring of integers modulo  $n$ ;

receiving a commitment  $R$  from a demonstrator, the commitment  $R$  having a value computed using the Chinese remainder method from a series of commitment components  $R_j$ , the commitment components  $R_j$  having a value such that:  $R_j = r_j^v \bmod p_j$  for  $j = 1, \dots, f$ , wherein  $r_1, \dots, r_f$  is a series of integers randomly chosen by the demonstrator;

choosing  $m$  challenges  $d_1, d_2, \dots, d_m$  randomly;

sending the challenges  $d_1, d_2, \dots, d_m$  to the demonstrator;

receiving a response  $D$  from the demonstrator, the response  $D$  being computed from a series of response components  $D_j$  using the Chinese remainder method, the response components  $D_j$  having a value such that:  $D_j = r_j \bullet Q_{1,j}^{d_1} \bullet Q_{2,j}^{d_2} \bullet \dots \bullet Q_{m,j}^{d_m} \bmod p_j$  for  $j=1,\dots,f$ , wherein  $Q_{i,j} = Q_i \bmod p_j$  for  $i=1,\dots,m$  and  $j=1,\dots,f$ ; and

determining that the demonstrator is authentic if the response  $D$  has a value such that:  $D^v \bullet G_1^{\varepsilon_1 d_1} \bullet G_2^{\varepsilon_2 d_2} \bullet \dots \bullet G_m^{\varepsilon_m d_m} \bmod n$  is equal to the commitment  $R$ , wherein, for  $i=1,\dots,m$ ,  $\varepsilon_i = +1$  in the case  $G_i \bullet Q_i^v = 1 \bmod n$  and  $\varepsilon_i = -1$  in the case  $G_i = Q_i^v \bmod n$ .

22. (Previously Presented) A computer implemented process comprising:

obtaining a set of one or more private values  $Q_1, Q_2, \dots, Q_m$  and respective public values  $G_1, G_2, \dots, G_m$ , each pair of values  $Q_i, G_i$  verifying either the equation  $G_i \bullet Q_i^v \equiv 1 \bmod n$  or the equation  $G_i \equiv Q_i^v \bmod n$ , wherein  $m$  is an integer greater than or equal to 1,  $i$  is an integer between 1 and  $m$ , and wherein  $n$  is a public integer equal to the product of  $f$  private prime factors designated by  $p_1, \dots, p_f$ , at least two of these prime factors being different from each other, wherein  $f$  is an integer greater than 1, and wherein  $v$  is a public exponent such that  $v = 2^k$ , and wherein  $k$  is a security parameter having an integer value greater than 1, and wherein each public value  $G_i$  for  $i=1,\dots,m$  is such that  $G_i \equiv g_i^2 \bmod n$ , wherein  $g_i$  for  $i=1,\dots,m$  is a base number having an integer value greater than 1 and smaller than each of the prime factors  $p_1, \dots, p_f$ , and  $g_i$  is a non-quadratic residue of the ring of integers modulo  $n$ ;

receiving a token  $T$  from a demonstrator, the token  $T$  having a value such that  $T = h(M, R)$ , wherein  $h$  is a hash function,  $M$  is a message received from the demonstrator, and  $R$  is a commitment having a value computed such that:  $R = r^v \bmod n$ , wherein  $r$  is an integer randomly chosen by the demonstrator;

choosing  $m$  challenges  $d_1, d_2, \dots, d_m$  randomly;

sending the challenges  $d_1, d_2, \dots, d_m$  to the demonstrator;

receiving a response  $D$  from the demonstrator, the response  $D$  having a value such that:

$$D = r \bullet Q_1^{d_1} \bullet Q_2^{d_2} \bullet \dots \bullet Q_m^{d_m} \bmod n ; \text{ and}$$

determining that the message  $M$  is authentic if the response  $D$  has a value such that:

$$h(M, D^v \bullet G_1^{\varepsilon_1 d_1} \bullet G_2^{\varepsilon_2 d_2} \bullet \dots \bullet G_m^{\varepsilon_m d_m} \bmod n) \text{ is equal to the token } T, \text{ wherein, for } i=1, \dots, m, \\ \varepsilon_i = +1 \text{ in the case } G_i \bullet Q_i^v = 1 \bmod n \text{ and } \varepsilon_i = -1 \text{ in the case } G_i = Q_i^v \bmod n .$$

23. (Previously Presented) A computer implemented process comprising:

obtaining a set of one or more private values  $Q_1, Q_2, \dots, Q_m$  and respective public values  $G_1, G_2, \dots, G_m$ , each pair of values  $Q_i, G_i$  verifying either the equation  $G_i \cdot Q_i^v \equiv 1 \bmod n$  or the equation  $G_i \equiv Q_i^v \bmod n$ , wherein  $m$  is an integer greater than or equal to 1,  $i$  is an integer between 1 and  $m$ , and wherein  $n$  is a public integer equal to the product of  $f$  private prime factors designated by  $p_1, \dots, p_f$ , at least two of these prime factors being different from each other, wherein  $f$  is an integer greater than 1, and wherein  $v$  is a public exponent such that  $v = 2^k$ , and wherein  $k$  is a security parameter having an integer value greater than 1, and wherein each public value  $G_i$  for  $i = 1, \dots, m$  is such that  $G_i \equiv g_i^2 \bmod n$ , wherein  $g_i$  for  $i = 1, \dots, m$  is a base number having an integer value greater than 1 and smaller than each of the prime factors  $p_1, \dots, p_f$ , and  $g_i$  is a non-quadratic residue of the ring of integers modulo  $n$ ;

receiving a token  $T$  from a demonstrator, the token  $T$  having a value such that  $T = h(M, R)$ , wherein  $h$  is a hash function,  $M$  is a message received from the demonstrator, and  $R$  is a commitment having a value computed out of commitment components  $R_j$  by using

the Chinese remainder method, the commitment components  $R_j$  having a value such that:  
 $R_j = r_j^v \bmod p_j$  for  $j=1,...,f$ , wherein  $r_1,...,r_f$  is a series of integers randomly chosen by the demonstrator;

choosing  $m$  challenges  $d_1, d_2, ..., d_m$  randomly;

sending the challenges  $d_1, d_2, ..., d_m$  to the demonstrator;

receiving a response  $D$  from the demonstrator, the response  $D$  being computed from a series of response components  $D_j$  using the Chinese remainder method, the response components  $D_j$  having a value such that:  $D_j = r_j \bullet Q_{1,j}^{d_1} \bullet Q_{2,j}^{d_2} \bullet ... \bullet Q_{m,j}^{d_m} \bmod p_j$  for  $j=1,...,f$ , wherein  $Q_{i,j} = Q_i \bmod p_j$  for  $i=1,...,m$  and  $j=1,...,f$ ; and

determining that the message  $M$  is authentic if the response  $D$  has a value such that:  
 $h(M, D^v \bullet G_1^{\varepsilon_1 d_1} \bullet G_2^{\varepsilon_2 d_2} \bullet ... \bullet G_m^{\varepsilon_m d_m} \bmod n)$  is equal to the token  $T$ , wherein, for  $i=1,...,m$ ,  
 $\varepsilon_i = +1$  in the case  $G_i \bullet Q_i^v = 1 \bmod n$  and  $\varepsilon_i = -1$  in the case  $G_i = Q_i^v \bmod n$ .

24. (Previously Presented) The computer implemented process according to claim 20, wherein the challenges are such that  $0 \leq d_i \leq 2^k - 1$  for  $i=1,...,m$ .

25. (Currently Amended) A computer implemented process comprising:

obtaining a set of one or more private values  $Q_1, Q_2, ..., Q_m$  and respective public values  $G_1, G_2, ..., G_m$ , each pair of values  $Q_i, G_i$  verifying either the equation  $G_i \cdot Q_i^v \equiv 1 \bmod n$  or the equation  $G_i \equiv Q_i^v \bmod n$ , wherein  $m$  is an integer greater than or equal to 1,  $i$  is an integer between 1 and  $m$ , and wherein  $n$  is a public integer equal to the product of  $f$  private prime factors designated by  $p_1, ..., p_f$ , at least two of these prime factors being different from each

other, wherein  $f$  is an integer greater than 1, and wherein  $v$  is a public exponent such that  $v = 2^k$ , and wherein  $k$  is a security parameter having an integer value greater than 1, and wherein each public value  $G_i$  for  $i = 1, \dots, m$  is such that  $G_i \equiv g_i^2 \pmod{n}$ , wherein  $g_i$  for  $i = 1, \dots, m$  is a base number having an integer value greater than 1 and smaller than each of the prime factors  $p_1, \dots, p_f$ , and  $g_i$  is a non-quadratic residue of the ring of integers modulo  $n$ ;

recording a message  $M$  to be signed;

choosing  $m$  integers  $r_i$  randomly, wherein  $i$  is an integer between 1 and  $m$ ;

computing commitments  $R_i$  having a value such that:  $R_i = r_i^v \pmod{n}$  for  $i = 1, \dots, m$ ;

computing a token  $T$  having a value such that  $T = h(M, R_1, R_2, \dots, R_m)$ , wherein  $h$  is a hash function producing a binary train consisting of  $m$  bits;

identifying the bits  $d_1, d_2, \dots, d_m$  of the token  $T$ ;

computing responses  $D_i = r_i \cdot Q_i^{d_i} \pmod{n}$  for  $i = 1, \dots, m$ ; and

~~making the token T and the responses  $D_i$  available to at least one of a public or a verifying entity~~

performing at least one of transmitting the token T and the response  $D_i$  to at least one verifying entity, or storing the token T and the response  $D_i$  on a database accessible to the public or to at least one verifying entity.

26. (Currently Amended) The computer implemented process according to claim 25, further comprising:

collecting the token  $T$  and the responses  $D_i$  for  $i = 1, \dots, m$ ; and

determining that the message  $M$  is authentic if the responses  ~~$D_i$~~  has  $D_i$  have a value such that:  ~~$h(M, D^v \cdot G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2} \cdot \dots \cdot G_m^{\varepsilon_m d_m} \bmod n)$~~

$$h(M, D_i^v \cdot G_1^{\varepsilon_1 d_1} \bmod n, D_2^v \cdot G_2^{\varepsilon_2 d_2} \bmod n, \dots, D_m^v \cdot G_m^{\varepsilon_m d_m} \bmod n)$$

is equal to the token  $T$ , wherein, for  $i = 1, \dots, m$ ,  $\varepsilon_i = +1$  in the case  $G_i \cdot Q_i^v = 1 \bmod n$  and  $\varepsilon_i = -1$  in the case  $G_i = Q_i^v \bmod n$ .

27-28. (Cancelled )

29. (Previously Presented) The computer implemented process according to claim 21, wherein the challenges are such that  $0 \leq d_i \leq 2^k - 1$  for  $i = 1, \dots, m$ .

30. (Previously Presented) The computer implemented process according to claim 22, wherein the challenges are such that  $0 \leq d_i \leq 2^k - 1$  for  $i = 1, \dots, m$ .

31. (Previously Presented) The computer implemented process according to claim 23, wherein the challenges are such that  $0 \leq d_i \leq 2^k - 1$  for  $i = 1, \dots, m$ .

32. (Previously Presented) A computer readable medium storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values  $Q_1, Q_2, \dots, Q_m$  and respective public values  $G_1, G_2, \dots, G_m$ , each pair of values  $Q_i, G_i$  verifying either the equation  $G_i \cdot Q_i^v \equiv 1 \bmod n$  or the equation  $G_i \equiv Q_i^v \bmod n$ , wherein  $m$  is an integer greater than or equal to 1,  $i$  is an integer between 1 and  $m$ , and wherein  $n$  is a public integer equal to the product of  $f$  private prime

factors designated by  $p_1, \dots, p_f$ , at least two of these prime factors being different from each other, wherein  $f$  is an integer greater than 1, and wherein  $v$  is a public exponent such that  $v = 2^k$ , and wherein  $k$  is a security parameter having an integer value greater than 1, and wherein each public value  $G_i$  for  $i = 1, \dots, m$  is such that  $G_i \equiv g_i^2 \pmod{n}$ , wherein  $g_i$  for  $i = 1, \dots, m$  is a base number having an integer value greater than 1 and smaller than each of the prime factors  $p_1, \dots, p_f$ , and  $g_i$  is a non-quadratic residue of the ring of integers modulo  $n$ ;

receiving a commitment  $R$  from a demonstrator, the commitment  $R$  having a value computed such that:  $R = r^v \pmod{n}$ , wherein  $r$  is an integer randomly chosen by the demonstrator;

choosing  $m$  challenges  $d_1, d_2, \dots, d_m$  randomly;

sending the challenges  $d_1, d_2, \dots, d_m$  to the demonstrator;

receiving a response  $D$  from the demonstrator, the response  $D$  having a value computed such that:  $D = r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \pmod{n}$ ; and

determining that the demonstrator is authentic if the response  $D$  has a value such that:  $D^v \cdot G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2} \cdot \dots \cdot G_m^{\varepsilon_m d_m} \pmod{n}$  is equal to the commitment  $R$ , wherein, for  $i = 1, \dots, m$ ,  $\varepsilon_i = +1$  in the case  $G_i \cdot Q_i^v = 1 \pmod{n}$  and  $\varepsilon_i = -1$  in the case  $G_i = Q_i^v \pmod{n}$ .

33. (Previously Presented) A computer readable medium storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values  $Q_1, Q_2, \dots, Q_m$  and respective public values  $G_1, G_2, \dots, G_m$ , each pair of values  $Q_i, G_i$  verifying either the equation  $G_i \cdot Q_i^v \equiv 1 \pmod{n}$  or the



equation  $G_i \equiv Q_i^v \pmod n$ , wherein  $m$  is an integer greater than or equal to 1,  $i$  is an integer between 1 and  $m$ , and wherein  $n$  is a public integer equal to the product of  $f$  private prime factors designated by  $p_1, \dots, p_f$ , at least two of these prime factors being different from each other, wherein  $f$  is an integer greater than 1, and wherein  $v$  is a public exponent such that  $v = 2^k$ , and wherein  $k$  is a security parameter having an integer value greater than 1, and wherein each public value  $G_i$  for  $i = 1, \dots, m$  is such that  $G_i \equiv g_i^2 \pmod n$ , wherein  $g_i$  for  $i = 1, \dots, m$  is a base number having an integer value greater than 1 and smaller than each of the prime factors  $p_1, \dots, p_f$ , and  $g_i$  is a non-quadratic residue of the ring of integers modulo  $n$ ;

receiving a commitment  $R$  from a demonstrator, the commitment  $R$  having a value computed using the Chinese remainder method from a series of commitment components  $R_j$ , the commitment components  $R_j$  having a value such that:  $R_j = r_j^v \pmod{p_j}$  for  $j = 1, \dots, f$ , wherein  $r_1, \dots, r_f$  is a series of integers randomly chosen by the demonstrator;

choosing  $m$  challenges  $d_1, d_2, \dots, d_m$  randomly;

sending the challenges  $d_1, d_2, \dots, d_m$  to the demonstrator;

receiving a response  $D$  from the demonstrator, the response  $D$  being computed from a series of response components  $D_j$  using the Chinese remainder method, the response components  $D_j$  having a value such that:  $D_j = r_j \cdot Q_{1,j}^{d_1} \cdot Q_{2,j}^{d_2} \cdot \dots \cdot Q_{m,j}^{d_m} \pmod{p_j}$  for  $j = 1, \dots, f$ , wherein  $Q_{i,j} = Q_i \pmod{p_j}$  for  $i = 1, \dots, m$  and  $j = 1, \dots, f$ ; and

determining that the demonstrator is authentic if the response  $D$  has a value such that:  $D^v \cdot G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2} \cdot \dots \cdot G_m^{\varepsilon_m d_m} \pmod n$  is equal to the commitment  $R$ , wherein, for  $i = 1, \dots, m$ ,  $\varepsilon_i = +1$  in the case  $G_i \cdot Q_i^v = 1 \pmod n$  and  $\varepsilon_i = -1$  in the case  $G_i = Q_i^v \pmod n$ .

34. (Previously Presented) A computer readable medium storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values  $Q_1, Q_2, \dots, Q_m$  and respective public values  $G_1, G_2, \dots, G_m$ , each pair of values  $Q_i, G_i$  verifying either the equation  $G_i \cdot Q_i^v \equiv 1 \pmod{n}$  or the equation  $G_i \equiv Q_i^v \pmod{n}$ , wherein  $m$  is an integer greater than or equal to 1,  $i$  is an integer between 1 and  $m$ , and wherein  $n$  is a public integer equal to the product of  $f$  private prime factors designated by  $p_1, \dots, p_f$ , at least two of these prime factors being different from each other, wherein  $f$  is an integer greater than 1, and wherein  $v$  is a public exponent such that  $v = 2^k$ , and wherein  $k$  is a security parameter having an integer value greater than 1, and wherein each public value  $G_i$  for  $i = 1, \dots, m$  is such that  $G_i \equiv g_i^2 \pmod{n}$ , wherein  $g_i$  for  $i = 1, \dots, m$  is a base number having an integer value greater than 1 and smaller than each of the prime factors  $p_1, \dots, p_f$ , and  $g_i$  is a non-quadratic residue of the ring of integers modulo  $n$ ;

receiving a token  $T$  from a demonstrator, the token  $T$  having a value such that  $T = h(M, R)$ , wherein  $h$  is a hash function,  $M$  is a message received from the demonstrator, and  $R$  is a commitment having a value computed such that:  $R = r^v \pmod{n}$ , wherein  $r$  is an integer randomly chosen by the demonstrator;

choosing  $m$  challenges  $d_1, d_2, \dots, d_m$  randomly;

sending the challenges  $d_1, d_2, \dots, d_m$  to the demonstrator;

receiving a response  $D$  from the demonstrator, the response  $D$  having a value such that:  
 $D = r \cdot Q_1^{d_1} Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \pmod{n}$ ; and

determining that the message  $M$  is authentic if the response  $D$  has a value such that:  
 $h(M, D^v \cdot G_1^{\epsilon_1 d_1} \cdot G_2^{\epsilon_2 d_2} \cdot \dots \cdot G_m^{\epsilon_m d_m} \pmod{n})$  is equal to the token  $T$ , wherein, for  $i = 1, \dots, m$ ,

$\varepsilon_i = +1$  in the case  $G_i \cdot Q_i^v = 1 \bmod n$  and  $\varepsilon_i = -1$  in the case  $G_i = Q_i^v \bmod n$ .

35. (Previously Presented) A computer readable medium storing instructions which when executed cause a processor to execute the following method:  
obtaining a set of one or more private values  $Q_1, Q_2, \dots, Q_m$  and respective public values  $G_1, G_2, \dots, G_m$ , each pair of values  $Q_i, G_i$  verifying either the equation  $G_i \cdot Q_i^v \equiv 1 \bmod n$  or the equation  $G_i \equiv Q_i^v \bmod n$ , wherein  $m$  is an integer greater than or equal to 1,  $i$  is an integer between 1 and  $m$ , and wherein  $n$  is a public integer equal to the product of  $f$  private prime factors designated by  $p_1, \dots, p_f$ , at least two of these prime factors being different from each other, wherein  $f$  is an integer greater than 1, and wherein  $v$  is a public exponent such that  $v = 2^k$ , and wherein  $k$  is a security parameter having an integer value greater than 1, and wherein each public value  $G_i$  for  $i = 1, \dots, m$  is such that  $G_i \equiv g_i^2 \bmod n$ , wherein  $g_i$  for  $i = 1, \dots, m$  is a base number having an integer value greater than 1 and smaller than each of the prime factors  $p_1, \dots, p_f$ , and  $g_i$  is a non-quadratic residue of the ring of integers modulo  $n$ ;

receiving a token  $T$  from a demonstrator, the token  $T$  having a value such that  $T = h(M, R)$ , wherein  $h$  is a hash function,  $M$  is a message received from the demonstrator, and  $R$  is a commitment having a value computed out of commitment components  $R_j$  by using the Chinese remainder method, the commitment components  $R_j$  having a value such that:  $R_j = r_j^v \bmod p_j$  for  $j = 1, \dots, f$ , wherein  $r_1, \dots, r_f$  is a series of integers randomly chosen by the demonstrator;

choosing  $m$  challenges  $d_1, d_2, \dots, d_m$  randomly;

sending the challenges  $d_1, d_2, \dots, d_m$  to the demonstrator;

receiving a response  $D$  from the demonstrator, the response  $D$  being computed from a

series of response components  $D_j$  using the Chinese remainder method, the response components  $D_j$  having a value such that:  $D_j = r_j \cdot Q_{1,j}^{d_1} \cdot Q_{2,j}^{d_2} \cdot \dots \cdot Q_{m,j}^{d_m} \bmod p_j$  for  $j=1,\dots,f$ , wherein  $Q_{i,j} = Q_i \bmod p_j$  for  $i=1,\dots,m$  and  $j=1,\dots,f$ ; and

determining that the message  $M$  is authentic if the response  $D$  has a value such that:  $h(M, D^v \cdot G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2} \cdot \dots \cdot G_m^{\varepsilon_m d_m} \bmod n)$  is equal to the token  $T$ , wherein, for  $i=1,\dots,m$ ,  $\varepsilon_i = +1$  in the case  $G_i \cdot Q_i^v = 1 \bmod n$  and  $\varepsilon_i = -1$  in the case  $G_i = Q_i^v \bmod n$ .

36. (Previously Presented) The computer readable medium according to claim 32, wherein the challenges are such that  $0 \leq d_i \leq 2^k - 1$  for  $i=1,\dots,m$ .

37. (Previously Presented) The computer readable medium according to claim 33, wherein the challenges are such that  $0 \leq d_i \leq 2^k - 1$  for  $i=1,\dots,m$ .

38. (Previously Presented) The computer readable medium according to claim 34, wherein the challenges are such that  $0 \leq d_i \leq 2^k - 1$  for  $i=1,\dots,m$ .

39. (Previously Presented) The computer readable medium according to claim 35, wherein the challenges are such that  $0 \leq d_i \leq 2^k - 1$  for  $i=1,\dots,m$ .

40. (Currently Amended) A computer readable medium storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values  $Q_1, Q_2, \dots, Q_m$  and respective public values  $G_1, G_2, \dots, G_m$ , each pair of values  $Q_i, G_i$  verifying either the equation  $G_i \cdot Q_i^v \equiv 1 \bmod n$  or the equation  $G_i \equiv Q_i^v \bmod n$ , wherein  $m$  is an integer greater than or equal to 1,  $i$  is an integer between 1 and  $m$ , and wherein  $n$  is a public integer equal to the product of  $f$  private prime factors designated by  $p_1, \dots, p_f$ , at least two of these prime factors being different from each

other, wherein  $f$  is an integer greater than 1, and wherein  $v$  is a public exponent such that  $v = 2^k$ , and wherein  $k$  is a security parameter having an integer value greater than 1, and wherein each public value  $G_i$  for  $i = 1, \dots, m$  is such that  $G_i \equiv g_i^2 \pmod{n}$ , wherein  $g_i$  for  $i = 1, \dots, m$  is a base number having an integer value greater than 1 and smaller than each of the prime factors  $p_1, \dots, p_f$ , and  $g_i$  is a non-quadratic residue of the ring of integers modulo  $n$ ;

recording a message  $M$  to be signed;

choosing  $m$  integers  $r_i$  randomly, wherein  $i$  is an integer between 1 and  $m$ ;

computing commitments  $R_i$  having a value such that:  $R_i = r_i^v \pmod{n}$  for  $i = 1, \dots, m$ ;

computing a token  $T$  having a value such that  $T = h(M, R_1, R_2, \dots, R_m)$ , wherein  $h$  is a hash function producing a binary train consisting of  $m$  bits;

identifying the bits  $d_1, d_2, \dots, d_m$  of the token  $T$ ;

computing responses  $D_i = r_i \cdot Q_i^{d_i} \pmod{n}$  for  $i = 1, \dots, m$ ; and

~~making the token T and the responses  $D_i$  available to at least one of a public or a verifying entity~~

performing at least one of transmitting the token T and the response  $D_i$  to at least one verifying entity, or storing the token T and the response  $D_i$  on a database accessible to the public or to at least one verifying entity.

41. (Currently Amended) The computer readable medium according to claim 40, the method further comprising:

collecting the token  $T$  and the responses  $D_i$  for  $i = 1, \dots, m$ ; and

determining that the message  $M$  is authentic if the responses  ~~$D$  has~~  $D_i$  have a value such that:  ~~$h(M, D^v \cdot G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2} \cdot \dots \cdot G_m^{\varepsilon_m d_m} \bmod n)$~~

$$\underline{h(M, D_i^v \cdot G_1^{\varepsilon_1 d_1} \bmod n, D_2^v \cdot G_2^{\varepsilon_2 d_2} \bmod n, \dots, D_m^v \cdot G_m^{\varepsilon_m d_m} \bmod n)}$$

is equal to the token  $T$ , wherein, for  $i = 1, \dots, m$ ,  $\varepsilon_i = +1$  in the case  $G_i \cdot Q_i^v = 1 \bmod n$  and  $\varepsilon_i = -1$  in the case  $G_i = Q_i^v \bmod n$ .